AMENDMENTS TO THE CLAIMS

1-33. (Cancelled).

34. (New) A method for detecting unauthorized intrusion in a computer network, comprising the steps of:

copying packets that are being transmitted in real-time over the computer network;

sorting the copied packets based on port type;

sending packets of a particular port type to one or more port modules, each port module being designed for processing packets of a single port type;

processing packets with each port module by reviewing and comparing information from various parts of each packet;

determining a presence and absence of port-specific activities based on each packet with each port module;

generating binary vectors representing the presence and absence of port-specific activities based on each packet with each port module;

assessing each binary vector and determining a level of expertise and deception for the port-specific activities represented by the binary vector with each port module;

outputting a behavioral rating from each port module in real-time based on the assessing and determining steps, the behavioral rating comprising at least two dimensions of deception and expertise.

35. (New) The method of Claim 34, further comprising combining behavioral ratings from a plurality of port modules.

36. (New) The method of Claim 34, further comprising determining if a threshold for a behavioral rating has been exceeded.

37. (New) The method of Claim 36, wherein if the threshold for a behavioral rating has been exceeded, then blocking user activity.

38. (New) The method of Claim 36, wherein if the threshold for a behavioral rating has been exceeded, then initiate a tracking of user activity.

39. (New) The method of Claim 34, wherein outputting a behavioral rating in real-time based on the determining step further comprises outputting a behavioral rating comprising at least one of a persistence and accuracy dimension.

40. (New) The method of Claim 34, further comprising mapping the behavioral rating on at least one two-dimensional grid.

41. (New) The method of Claim 34, further comprising generating a profile a user based upon monitored behavioral measures.

42. (New) The method of Claim 34, wherein the step of assessing each binary vector and determining a level of expertise and deception is carried out utilizing a back propagation network.

43. (New) The method of Claim 42, wherein the back propagation network includes psychological assessment information.

44. (New) The method of Claim 34, wherein the behavioral rating comprises one of high deception/high expertise, high deception/low expertise, low deception/high expertise and low deception/low expertise.

45. (New) The method of Claim 37, wherein the blocking user activity comprises sending a blocking command to a firewall for blocking further network access.

46. (New) The method of Claim 37, wherein blocking user activity comprises a loss of a connection between a user and the computer network and storage of all relevant session data up to the point of forced loss.

47. (New) The method of Claim 38, wherein tracking of user activity comprises storing activity information in a database that may be used to provide evidence of an intruder's harmful intent activities.

48. (New) A system for preventing unauthorized intrusion in a network system, comprising:

a traffic sorter for sorting copied packets based on port type;

an activity monitor operatively coupled to the traffic sorter, the activity monitor comprising a plurality of port modules, each port module being designed for processing packets of a single type and processing packets by reviewing and comparing information from various parts of each packet and determining a presence and absence of port-specific activities based on each packet, each port module outputting a behavioral rating in real-time based, the behavioral rating comprising at least two dimensions of deception and expertise;

an inter-port fusion module operatively coupled to the activity monitor for grouping behavioral ratings received from the port modules of the activity monitor; and

an outcome director operatively coupled to the inter-port fusion monitor that determines whether to block or track user activities based upon the behavioral ratings received from the inter-port fusion module.

49. (New) The system of Claim 48, wherein each port module generates binary vectors representing the presence and absence of port-specific activities based on each packet.

50. (New) The system of Claim 49, wherein each port module assesses each binary vector and determines a level of expertise and deception for the port-specific activities represented by the binary vector.

51. (New) A computer program product, comprising:

a computer usable medium having computer readable code embodied therein for preventing unauthorized intrusion into a computer network, the computer program product comprising:

computer readable program code configured to cause a computer to copy packets that are being transmitted in real-time over the computer network;

computer readable program code configured to cause the computer to sort the copied packets based on port type;

computer readable program code configured to cause the computer to process packets of a single port type;

computer readable program code configured to cause the computer to process packets by reviewing and comparing information from various parts of each packet;

computer readable program code configured to cause the computer to determine a presence and absence of port-specific activities based on the review and comparison of each packet;

computer readable program code configured to cause the computer to generate binary vectors representing the presence and absence of port-specific activities based on each packet;

computer readable program code configured to cause the computer to assess each binary vector and determine a level of expertise and deception for the port-specific activities represented by the binary vector; and

computer readable program code configured to cause the computer to output a behavioral rating from each port module in real-time based on the determining step, the behavioral rating comprising at least two dimensions of deception and expertise.

52. (New) The computer program product of Claim 51, wherein the computer readable program code is configured to cause the computer to combine behavioral ratings from a plurality of port modules.

53. (New) The computer program product of Claim 51, wherein the computer readable program code is configured to cause the computer to determine if a threshold for a behavioral rating has been exceeded [S560/580].

[The remainder of this page has been intentionally left blank.]